PROJECT 25 – INTEROPERABILITY AND SECURITY

Jim Downes

Chair, Project 25 Technology Interest Group

Department of Homeland Security, Office of Emergency Communications

February 9, 2011

Background – Why Project 25

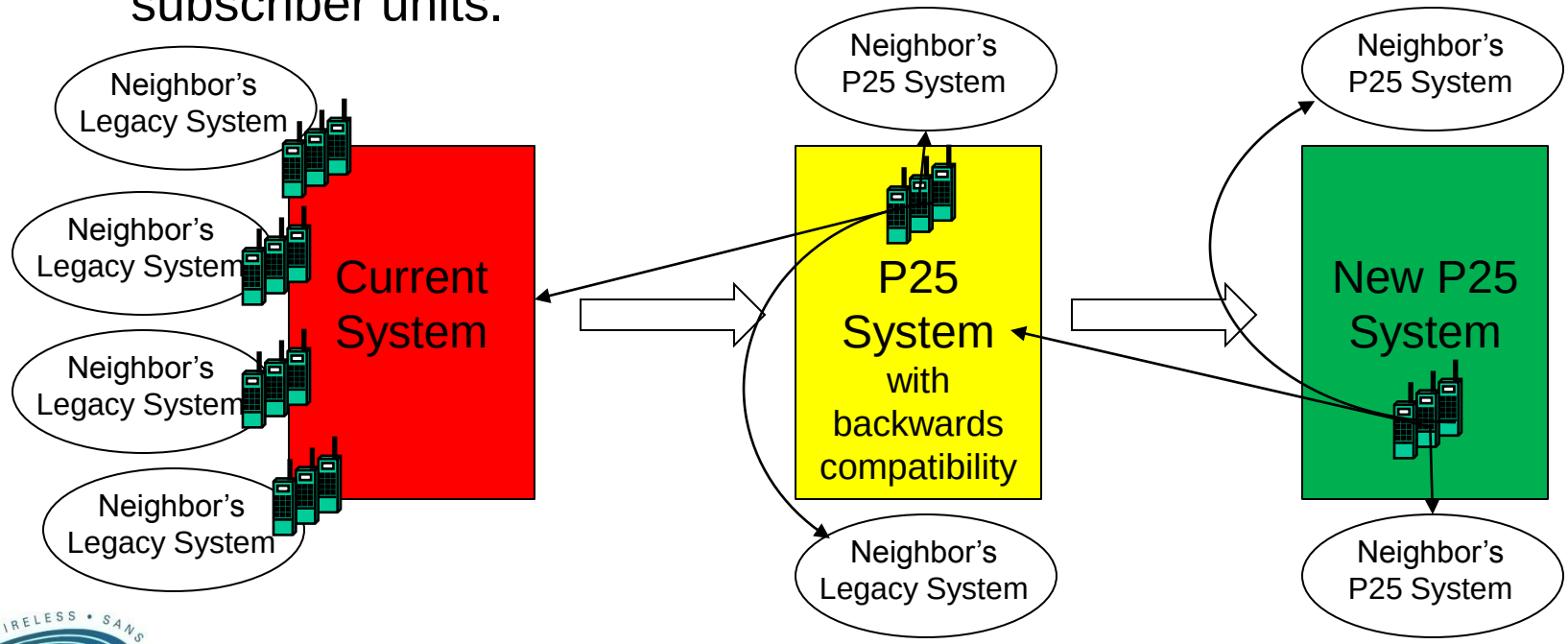
- Project 25 is the only Public Safety user-driven, land mobile radio standard that currently exists
- User participation includes all levels of government (federal, state, local, tribal and provincial)
- Project 25 defines messages and procedures for eleven interfaces as well as several key features and functions necessary to complete the public safety mission
- Project 25 is continually evolving to include more features and functions as well as new technologies as they become standardized
- US Federal grant guidance requires Project 25 compliant equipment for new implementations
- TIA has developed and published over sixty-four standard documents that define each interface. Over 125 documents have been developed and published supporting the standards and features offered in the Project 25 suite

P25 Procurement Best Practices

- The various interfaces and features of Project 25 are established in a multitude of Project 25/TIA standards. A generic procurement statement requiring Project 25 is not sufficient. Referencing Project 25 generically does not replace sound engineering best practices to ensure public safety requirements are met.
- When implementing an encryption algorithm, please remember that the only P25 supported algorithms are the Data Encryption Standard – Output Feedback (DES-OFB) and the Advanced Encryption Standard (AES). Proprietary encryption/protection schemes are not standardized and further complicate interoperability.
- When implementing proprietary solutions, include language in your procurement specification requiring a migration path to standards compliant technologies and feature sets. Remember to build the migration into your system life cycle costs for future standards based solutions.

P25 Procurement Best Practices

- Evaluate your current needs to include your surrounding jurisdictions. Optimal interoperability may be a multi-staged migration.
- Be mindful of implementing proprietary feature sets that may require a specific manufacturer's service offering in future iterations. This is true for both infrastructure options as well as subscriber units.



P25 Myths and Reality

- Myth: *"Project 25 is an old technology that has already passed its prime."*
  - **Best Practice**: Project 25 has been in development over 21 years, but during that time, the standards have been updated, reaffirmed, or completely revised several times. The TIA engineering manual requires that every published standard document be reviewed and reaffirmed, updated or withdrawn every five years at a minimum. TIA standard documents are often updated more often as new technologies, clarifications or user requirements change.
- Myth: *"Project 25 is only available from a single vendor."*
  - **Best Practice**: Actually, that used to be a true statement for infrastructure. However, the following slide will give you an idea of the number of vendors that are participating in the Project 25 development process as well as their respective equipment offerings.

Project 25 Equipment Manufacturers

PTIG Manufacturer	Stations / Repeaters	Mobiles	Portables	Consoles	Networks	P25 Software	Test Equipment	Systems Integration	Consultant Services
Aecom									
Aeroflex									
Avtec									
CadStar									
Cobham - Wulfsberg									
Daniels									
Datron									
DVSI									
EADS									
E F Johnson									
Etherstack									
Federal Engineering									
General Dynamics									
Genesis Group									
Harris									
iCOM America									
Incident Specialists									
Kenwood									
Midland									
Motorola									
Pantel									
PowerTrunk									
Raytheon JPS									
RELM Wireless									
Simoco									
Survey Technology									
TAIT									
Technisonics									
Thales									
Vertex Standard									
Zetron									
	11	14	13	7	8	3	5	12	8

P25 Myths and Reality

- Myth: *"It is sufficient to just reference P25 in my procurement document."*
  - **Best Practice**: When specifying P25 in your procurement documentation, make sure you include the specific P25 interfaces, features and functions you and your agency require.
- Myth: *"The P25 CAP does not provide benefits to Federal agencies because their funding sources do not include grants."*
  - **Best Practice**: While the P25 CAP is heavily referenced in several grant guidance documents, it was developed to provide a baseline of P25 compliance. The P25 CAP CABs are beneficial to all levels of government regardless of their funding source.
- Myth: *"The P25 CAP does not cover all of the interfaces."*
  - **Best Practice**: The P25 CAP has published a number of CABs covering the Common Air Interface for Project 25 Phase 1 and the ISSI . Additional Recommended Compliance Assessment Tests (RCATs) and CABs are being developed as resources become available. Ultimately CABs will be developed for each interface.

P25 Myths and Reality

- Myth: *"Referencing the P25 CAP is all I need in my procurement documents."*
  - **Best Practice**: The P25 CAP CABs are only a subset of the performance, conformance and interoperability tests associated with a particular interface and/or feature. The P25 CAP does not replace sound engineering best practices to ensure public safety requirements are met. In some cases, P25 compliance may include the complete set of tests for your agency's implementation. Additionally, your system may or may not implement multiple P25 interfaces which may or may not be covered by the P25 CAP.
- Myth: *"I don't need high level encryption. I'm only trying to prevent scanners from hearing my conversations."*
  - **Best Practice**: Low-tier encryption algorithms, or even digital privacy options, may create a false sense of security for users. NIST has shown that algorithms shorter than 112 bits in key length are prone to real-time exhaustive key search attacks. P25 supports both AES 256-bit keys (recommended algorithm) and DES-OFB keys for backwards compatibility and interoperability.

P25 Myths and Reality

- Myth: *“P25 Equipment is cost prohibitive.”*
  - **Best Practice**: P25 radios are available in a number of configurations ranging in price from your basic model all the way to the fully loaded feature set. Not all P25 radios require a full feature set to be P25 compliant. Proprietary solutions may end up costing you many times the expense if you are not careful.

P25 Resources

- Project 25 Technology Interest Group
  - http://www.project25.org/
  - Contact: Bill Pagones (director@project25.org)
- SAFECOM Grant Guidance
  - http://www.safecomprogram.gov/SAFECOM/grant/default.htm
- P25 CAP
  - http://www.safecomprogram.gov/SAFECOM/currentprojects/project25cap/project25cap.htm
  - Responder Knowledge Base: www.rkb.us
- Telecommunications Industry Association
  - Project 25 For Government Series
    - Contact Ronda Coulter: rcoulter@tiaonline.org
- Project 25 User Needs
  - Contact: Scott Bradford (sbradford@mt.gov)